

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of detecting a denial of service attack at a network server, comprising: ~~the steps of~~
counting ~~[[the]]~~ a number of inbound packets and ~~[[the]]~~ a number of discarded packets ~~[[X]]~~ in a specified interval,
~~responsive to [[if]] the number of discarded packets [[X]] in the specified interval [[exceeds]] exceeding a specified minimum $X(\text{MIN})$, [[then]] calculating [[the]] a percentage of discarded packets, $R = X$ wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and~~
~~responsive to the percentage of discarded packets exceeding if R exceeds a specified threshold, [[then]] setting a denial of service event marker.~~
2. (Currently Amended) The method of claim 1, further comprising: ~~the step of~~
collecting ~~relevant~~ inbound packet information to further characterize the denial of service attack.
3. (Currently Amended) The method of claim 2, wherein ~~the step of~~ collecting the relevant inbound packet information further comprises:
initiating a flood monitoring process that is executed at designated ~~a specified~~ intervals to collect the ~~relevant~~ inbound packet information while the denial of service attack is in progress.
4. (Currently Amended) The method of claim 3, wherein the flood monitoring process comprises:
resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum, $X(\text{MIN2})$, ~~wherein $X(\text{MIN2})$ may or may not equal $X(\text{MIN})$.~~
5. (Currently Amended) The method of claim 3, wherein the flood monitoring process comprises:
resetting the denial of service event marker if ~~[[the]]~~ a rate of discarded packets in the specified interval before execution of the flood monitoring process is less than a second specified threshold.

6. (Currently Amended) The method of claim 4, ~~or claim 5~~ further comprising: ~~the further step of~~ collecting ~~the relevant~~ inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.
7. (Currently Amended) The method of claim 6, wherein the ~~collected~~ inbound packet information includes at least one of: ~~can consist of one or more of the following:~~
- a) ~~[[the]]~~ a number of inbound packets in ~~[[the]]~~ a last interval;
 - b) ~~[[the]]~~ a number of discarded packets in ~~[[the]]~~ a last interval;
 - c) ~~[[the]]~~ a packet discard rate;
 - d) ~~[[the]]~~ a most frequent discard protocol type;
 - e) ~~[[the]]~~ a most frequent discard ~~discard~~ type; and
 - f) ~~[[the]]~~ a media access control (MAC) address of ~~[[the]]~~ an immediately prior packet hop.
8. (Currently Amended) The method of claim 3, wherein the flood monitoring process comprises: determining if the ~~[[flood]]~~ denial of service attack is still in progress by comparing ~~[[the]]~~ packets discarded in ~~[[the]]~~ a last interval with the number of inbound packets, and maintaining ~~the scheduling of~~ the flood monitoring process if the denial of service attack is still in progress.
9. (Currently Amended) The method of claim 8, further comprising: collecting ~~relevant~~ inbound packet information for the last interval.
10. (New) The method of claim 5, further comprising: collecting additional inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.